CLAIMS

1. A method for providing computer security, comprising:

providing an executable associated with a static state;

determining whether the executable meets a predetermined criterion; and

associating a risk level with the criterion, if it is determined that the executable meets the predetermined criterion;

wherein determining whether the executable meets a predetermined criterion does not compare the executable with a virus signature.

2. A method for providing computer security as recited in Claim 1,wherein the risk level indicates a level of potential risk that will be brought by operating the executable.

3. A method for providing computer security as recited in Claim 1, wherein the risk level indicates how much risk the executable presents.

4. A method for providing computer security as recited in Claim 1, wherein the predetermined criterion includes a configuration criterion.

5. A method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable is configured as a service.

6. A method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable is configured to run under a highly privileged account.

7. A method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable is installed via a standard procedure.

8. A method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has sufficient access control.

9. A method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable is recent.

10. A method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable is signed.

11. A method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has a modified date different from created date.

12. A method for providing computer security as recited in Claim 1, wherein the predetermined criterion includes a capability criterion.

13. A method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has networking capability.

14. A method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has privilege manipulation capability.

15. A method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has remote process capability.

16. A method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has process launching capability.

17. A method for providing computer security as recited in Claim 1, wherein the predetermined criterion is used to determine whether the executable has secure coding violation.

18. A method for providing computer security as recited in Claim 1, further comprising associating with the executable a risk type indicating a type of risk to which the executable is vulnerable.

19. A method for providing computer security as recited in Claim 1, wherein the predetermined criterion is a first predetermined criterion, and the method further includes determining whether a process associated with the executable meets a second predetermined criterion.

20. A method for providing computer security as recited in Claim 1, wherein the predetermined criterion is a first predetermined criterion, and the method further includes determining whether a process that is a running instance of the executable meets a second predetermined criterion.

21. A method for providing computer security as recited in Claim 1, wherein the predetermined criterion is a first predetermined criterion, and the method further includes

determining whether a process associated with the executable meets a second predetermined criterion, the process being a process that is currently operating.

22. A method for providing computer security as recited in Claim 1, wherein the predetermined criterion is a first predetermined criterion, and the method further includes determining whether a process associated with the executable meets a second predetermined criterion, wherein the second predetermined criterion includes a configuration criterion.

23. A method for providing computer security as recited in Claim 1, wherein the predetermined criterion is a first predetermined criterion, and the method further includes determining whether a process associated with the executable meets a second predetermined criterion, wherein the second predetermined criterion is used to determine whether the process is operating with a higher effective privilege than it is configured.

24. A method for providing computer security as recited in Claim 1, wherein the predetermined criterion is a first predetermined criterion, and the method further includes determining whether a process associated with the executable meets a second predetermined criterion, wherein the second predetermined criterion is used to determine whether the process has higher privilege than it is warranted.

25. A method for providing computer security as recited in Claim 1, wherein the predetermined criterion is a first predetermined criterion, and the method further includes determining whether a process associated with the executable meets a second predetermined criterion, wherein the second predetermined criterion is used to determine whether the process loads a dynamic library during its operation.

26. A method for providing computer security as recited in Claim 1, wherein the predetermined criterion is a first predetermined criterion, and the method further includes determining whether a process associated with the executable meets a second predetermined criterion, wherein the second predetermined criterion includes a capability criterion.

27. A method for providing computer security as recited in Claim 1, wherein the predetermined criterion is a first predetermined criterion, and the method further includes determining whether a process associated with the executable meets a second predetermined criterion, wherein the second predetermined criterion is used to determine whether the process owns a system object that does not have sufficient access control.

28. A method for providing computer security as recited in Claim 1, wherein the predetermined criterion is a first predetermined criterion, and the method further includes determining whether a process associated with the executable meets a second predetermined criterion, wherein the second predetermined criterion is used to determine whether the process has networking capability.

29. A method for providing computer security as recited in Claim 1, further comprising analyzing historical evidence.

30. A method for providing computer security as recited in Claim 1, further comprising analyzing historical evidence, wherein the historical evidence includes a record of activities.

31. A method for providing computer security as recited in Claim 1, further comprising analyzing historical evidence, wherein the historical evidence includes a log file.

32. A method for providing computer security as recited in Claim 1, further comprising analyzing historical evidence, wherein the historical evidence includes a system optimization file.

33. A method for providing computer security as recited in Claim 1, further comprising analyzing historical evidence, wherein the historical evidence includes a crash dump file.

34. A method for providing computer security as recited in Claim 1, further comprising analyzing historical evidence, wherein the historical evidence includes a prefetch file.

35. A method for providing computer security as recited in Claim 1, further comprising performing a dynamic risk analysis.

36. A method for providing computer security as recited in Claim 1, further comprising determining whether an action is required.

37. A system for providing computer security, comprising:

a processor configured to:

provide an executable associated with a static state;

determine whether the executable meets a predetermined criterion; and

associate a risk level with the criterion, if it is determined that the executable meets the predetermined criterion;

wherein determining whether the executable meets a predetermined criterion does not compare the executable with a virus signature; and

a memory coupled with the processor, configured to provide the processor with instructions.

38. A computer program product for providing computer security , the computer program product being embodied in a computer readable medium and comprising computer instructions for:

providing an executable associated with a static state;

determining whether the executable meets a predetermined criterion; and

associating a risk level with the criterion, if it is determined that the executable meets the predetermined criterion;

wherein determining whether the executable meets a predetermined criterion does not compare the executable with a virus signature.